

REMARKS

The present application was filed on December 14, 1999, with claims 1-59. Claims 1-59 are currently pending in the application. Claims 1, 41 and 54 are the independent claims.

Claims 1-12, 15-17, 41-51 and 54-56 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,269,149 (hereinafter "Hassell"). Claims 13, 14, 18-21, 52, 53 and 57-59 are rejected under 35 U.S.C. §103(a) as being unpatentable over Hassell in view of U.S. Patent No. 6,327,660 (hereinafter "Patel"). Claims 22-40 are indicated as containing allowable subject matter.

In this response, Applicant respectfully traverses the §102(e) and §103(a) rejections. Applicant requests reconsideration of the present application in view of the following remarks.

With regard to the §102(e) rejection, Applicant initially notes that the Manual of Patent Examining Procedure (MPEP), Eight Edition, August 2001, §2131, specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The present invention is generally directed to methods for establishing secure communications between users employing endpoints in a system which includes one or more security zones each having an associated Zone Keeper. An arrangement of this type is referred to in the specification as a dual-tier security architecture. With reference to independent claim 1, this claim more particularly specifies that a first Zone Keeper, associated with a first security zone including a first endpoint, determines whether a requested secure communication, between a caller utilizing the first endpoint and a callee utilizing a second endpoint, is an intra-zone or an inter-zone communication. If the requested communication is an intra-zone communication, both the first and second endpoints are in the same security zone, and the first Zone Keeper in conjunction with the first and second endpoints in the first security zone establishes the secure communication between the caller and the callee. If the requested communication is an inter-zone communication, the first

and second endpoints are in first and second security zones, respectively, the first Zone Keeper sends a request message to a second Zone Keeper associated with the second security zone, and the secure communication is established between the zones utilizing the first and second Zone Keepers and the associated first and second endpoints.

The Hassell reference relied upon by the Examiner fails to meet the above-noted limitations of independent claim 1. For example, there is no mention whatsoever in Hassell regarding the claimed security zones, each having an associated Zone Keeper, or the claimed determination as to whether a given requested secure communication constitutes an intra-zone or inter-zone communication. Thus, Hassell fails to teach or suggest a dual-tier security architecture of the type claimed.

The Examiner at page 16, lines 15-17, of the final Office Action argues that such a reference to a dual-tier security architecture “does not even address in [sic] the claim language.” As indicated above, claim 1, by way of example, includes limitations relating to intra-zone communication and inter-zone communication. Intra-zone communications are handled by a first Zone Keeper in a corresponding first security zone. Inter-zone communications, on the other hand, involve particular interactions between a first Zone Keeper associated with a first security zone and a second Zone Keeper associated with a second security zone. The specification makes clear that this type of security architecture, involving distinct handling of intra-zone communications and inter-zone communications from a security standpoint, is referred to as a dual-tier security architecture. See the specification at, for example, page 1, lines 21-29, and page 3, lines 14-15. Accordingly, claim 1 does describe a dual-tier security architecture, by its references to distinct handling of intra-zone and inter-zone communications, and to first and second security zones and their respective first and second Zone Keepers.

In formulating the §103(a) rejection, the Examiner specifically relies on the teachings in Hassell at column 2, line 60, to column 3, line 20. This portion of the cited reference provides as follows:

In accordance with another aspect of the present invention, a method for establishing a secured telecommunications link between a calling party and a called party is provided.

In accordance with this aspect of the invention, the method includes the steps of receiving a calling from a remote user, identifying the caller identification number, and using caller identification number to access a lookup table. The method further includes the steps of determining whether a profile exists in the lookup table that corresponds to the identified caller identification element. If so, the method further confirms from information provided in the lookup table, whether that user is entitled to access the system. If so, then the method directs the system to establish the connection with the remote user. In a preferred embodiment, the system may provide an added level of security by requiring the remote user to enter a password, as well.

Preferably, this aspect of the invention includes the steps of receiving a signal from a calling party that is requesting the establishment of a communication link, and examining call setup information within the received signal for the second calling party to identify the telephone number of the second calling party. The method further includes the steps of accessing a memory storage area using the telephone number of the second calling party to retrieve information relating to the calling party, and evaluating security data of the retrieved information. If the security data permits the establishment of a connection, then the method establishes a communication link with the calling party.

It is readily apparent that the relied-upon passages quoted above fail to make any reference to security zones or a determination as to whether a given communication is an intra-zone or inter-zone communication. By treating all communications in substantially the same manner, without regard to the relationship of the associated endpoints to one or more security zones, Hassell actually teaches away from the invention as recited in claim 1.

The Examiner also makes reference to column 4, lines 29-33, and to the drawing in FIG. 1 of Hassell which shows a first or calling endpoint 12 and a second or called endpoint 14 communicating over a network 16. Again, there is no teaching or suggestion here or anywhere else in Hassell regarding endpoints 12 or 14 potentially being in different security zones associated with respective Zone Keepers, nor any determination as to whether a given requested secure communication is an intra-zone communication or an inter-zone communication.

In the final Office Action, at page 15, last paragraph, to page 16, first paragraph, the Examiner relies on the teachings in column 7, lines 11-20, and column 1, lines 35-67, of Hassell. The teachings from column 7, lines 11-20, provide as follows:

Turning now to FIG. 3, a flowchart is provided that depicts the top-level operation of the prioritization aspect of the present invention. Specifically, upon receiving an incoming call, the system validates the call by way of identifying the caller ID (at step 60). This validation step, having been briefly described above, will be described in more detail in connection with FIG. 4. Upon validating the caller ID, the system then determines from an internal database (at step 62) whether it has a prioritization profile for this particular caller ID. If not, it rejects the incoming call (step 64).

The Examiner argues that the “system” referred to in this passage corresponds to one of the claimed Zone Keepers. Apparently, the “system” referred to in this passage is the system shown in FIG. 1 of Hassell, which includes calling endpoint 12, called endpoint 14, and the network 16 over which they communicate. However, there is no indication in Hassell to the effect that there are multiple such systems which interact in the manner set forth in claim 1 to establish secure inter-zone communications.

The teachings from column 1, lines 35-67, of Hassell, provide as follows:

There are, however, various shortcomings in the present state of the art, including the handling of fault detection, security, and call prioritization. Mechanisms are well known for identifying and notifying a user of a line breakage or other fault condition existing in the link between endpoints. However, endpoint equipment often responds by rerouting all data on a particular line, as opposed to on the affected data. For example, suppose one endpoint of a telecommunications network interfaces to a local area network (e.g. a corporate network) and the telecommunications link communicating with the endpoint is a high capacity T1 line. If the endpoint detects a fault or breakage in any channel(s) of the T1 line, present systems operate to reroute the entirety of the data traffic across that T1 line through another port,

whether that be a secondary T1 line or an alternative backup link. However, fractional or partial line faults are often encountered, making such a global rerouting of data wasteful and unnecessary. For example, data transmitted across a frame relay network (e.g., packet-switched data) often suffers only a partial fault, or a network breakage at some intermediate point across which only a portion of the data to the ultimate endpoint traverses.

Another shortcoming noted in present state of the art systems relates to security. In keeping with the previous example of telecommunications network endpoint being connected to a local area network, there is a tremendous need for providing a secured entry from any caller outside the local area network to access the network by way of, for example, a dial-up connection. Frequently security issues, such as this one, are handled by password protection. In such systems, dial-up users are required to provide a password for access to the network.

Again, this fails to provide any teaching or suggestion regarding the separation of a system into security zones, each including a corresponding Zone Keeper, as claimed. At best, it simply indicates the well-known notion that a caller may be required to enter a password to obtain access to a local area network. This is not what Applicant is attempting to claim, as is readily apparent from even a cursory review of claim 1.

Applicant also notes that the technique that Hassell uses to provide secure communications is described generally at column 2, line 59, to column 3, line 8, which portion was previously quoted above. There is no mention in this teaching regarding the separation of a system into security zones, each with a corresponding Zone Keeper, and interaction between the Zone Keepers in the manner specified in claim 1. Accordingly, the Hassell system fails to provide the advantages of the claimed invention in terms of its ability to facilitate intra-zone and inter-zone secure communication. See the specification at, for example, page 1, lines 21-29, and page 2, lines 21-25.

Since independent claim 1 includes limitations which are not disclosed in Hassell, that reference is not anticipatory of claim 1.

Similarly, Hassell fails to teach or suggest the security zone, Zone Keeper and communication protocol limitations of independent claims 41 and 54, and in fact teaches away from

the claimed arrangements by teaching to use different arrangements than those specifically claimed in order to set up a secure communication between endpoints.

The rejected dependent claims are believed allowable for at least the reasons identified above with regard to their respective independent claims, and are also believed to define separately-patentable subject matter.

With regard to the §103(a) rejection, a proper *prima facie* case of obviousness requires that the cited references when combined must “teach or suggest all the claim limitations,” and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references or to modify the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

The Patel reference cited by the Examiner fails to overcome the fundamental deficiencies of Hassell as applied to the independent claims. Thus, the proposed combination fails to “teach or suggest all the claim limitations” as is required for establishment of a proper *prima facie* case.

Furthermore, the Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination “must be based on objective evidence of record” and that “this precedent has been reinforced in myriad decisions, and cannot be dispensed with.” In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). The Federal Circuit has further stated that “conclusory statements” by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved “on subjective belief and unknown authority.” Id. at 1343-1344. Applicant submits that the Examiner has failed to provide any objective evidence of motivation to combine Hassell and Patel, or to modify their teachings, to meet the claim limitations in question. The particular statement provided by the Examiner is on page 14, last paragraph, to page 15, first paragraph, of the final Office Action, and is as follows:

The ordinary skilled person would have been motivated to add such security association 700 (in Hassell) because a communication channel is considered to be “secure” when (i) the modification of data transmitted through the communication channel can be detected, and (ii) the source of the transmitted data can be authenticated, and/or the

confidentiality of the transmitted data is protected. Cryptographic techniques such as digital certificates, digital signatures, and the encryption/decryption of data are used to secure a communication channel.

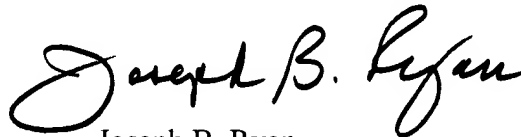
There is no objective evidence of motivation here. The Examiner has instead provided only a conclusory statement of obviousness based on the type of "subjective belief and unknown authority" that the Federal Circuit has indicated is insufficient to support an obviousness rejection. At best, the quoted statement simply indicates the well-known fact that cryptographic techniques can be used to provide secure communication. This alone is insufficient evidence of motivation to combine the particular cryptographic techniques of Patel, which are specifically designed for use in a "pre-boot environment," that is, for use prior to booting of an operating system, with the communication processing techniques of Hassell. In a sense, Hassell and Patel are non-analogous because Hassell bears no relation to the pre-boot environment while Patel is specifically directed to that context. Accordingly, additional objective motivation to combine Hassell and Patel is required to support a *prima facie* case of obviousness, beyond the mere notion that cryptographic techniques can be used to provide secure communication.

The §103(a) rejection is therefore believed to be improper and should be withdrawn.

In view of the above, Applicant believes that claims 1-59 are in condition for allowance, and respectfully requests withdrawal of the §102(e) and §103(a) rejections.

As indicated previously, a Notice of Appeal is submitted concurrently herewith.

Respectfully submitted,

A handwritten signature in black ink that reads "Joseph B. Ryan". The signature is written in a cursive, flowing style with a large initial 'J'.

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

Date: January 19, 2005

Enclosure(s): Notice of Appeal